CheatSheet con 400 comandos para GNU/Linux que deberías saber

By Leo Romero 4 may 2013 18:42 CheatSheet, GNU/Linux, Hack Tips, Linux OS, Tips, Trucos



Índice:

Información del sistema

1. **arch**: mostrar la arquitectura de la máquina (1).
2. **uname -m**: mostrar la arquitectura de la máquina (2).
3. **uname -r**: mostrar la versión del kernel usado.
4. **dmidecode -q**: mostrar los componentes (hardware) del sistema.
5. **hdparm -i /dev/hda**: mostrar las características de un disco duro.
6. **hdparm -tT /dev/sda**: realizar prueba de lectura en un disco duro.
7. **cat /proc/cpuinfo**: mostrar información de la CPU.

Buscar


Popular Posts


Las 20 herramientas de hacking más populares del 2023
En un ranking elaborado por Kitploit , nos muestran las 20 herramientas más populares (con más visitas) durante el 2022. Es una lista que m...


Hackeando un Banco 3 ["Hackear" 14.000+ Tarjetas de Crédito (Carding)]
Recientemente en la prensa chilena ha causado bastante estragos diferentes noticias relacionadas con la mala seguridad informática co...


Crack MD5, SHA1, MySQL, NTLM Free Online!
Hace algún tiempo salió InsidePro Hash Finder un buscador de hashes másivo, gratuito y online donde se pueden encontrar hasta 25 mil h...


Las 20 herramientas de hacking más populares del 2020
En un ranking elaborado por Kitploit , nos muestran las 20 herramientas más populares (con más visitas) durante el 2020. Es una lista que m...

Blog Archive

- ► 2023 (2)
- ► 2022 (1)
- ► 2021 (2)
- ► 2020 (2)
- ► 2019 (6)
- ► 2018 (8)
- ► 2017 (3)
- ► 2016 (5)
- ► 2015 (8)
- ► 2014 (15)
- ▼ 2013 (40)
  - ► diciembre (3)
  - ► noviembre (4)
  - ► octubre (6)
  - ► septiembre (1)
  - ► agosto (3)
  - ► julio (2)
  - ► junio (2)
  - ▼ mayo (1)
    - CheatSheet con 400 comandos para GNU/Linux que deb...
  - ► abril (3)
  - ► marzo (4)
  - ► febrero (5)



8. **cat /proc/interrupts**: mostrar las interrupciones.
9. **cat /proc/meminfo**: verificar el uso de memoria.
10. **cat /proc/swaps**: mostrar ficheros swap.
11. **cat /proc/version**: mostrar la versión del kernel.
12. **cat /proc/net/dev**: mostrar adaptadores de red y estadísticas.
13. **cat /proc/mounts**: mostrar el sistema de ficheros montado.
14. **lspci -tv**: mostrar los dispositivos PCI.
15. **lsusb -tv**: mostrar los dispositivos USB.
16. **date**: mostrar la fecha del sistema.
17. **cal 2011**: mostrar el almanaque de 2011.
18. **cal 07 2011**: mostrar el almanaque para el mes julio de 2011.
19. **date 041217002011.00**: colocar (declarar, ajustar) fecha y hora.
20. **clock -w**: guardar los cambios de fecha en la BIOS.

Apagar (Reiniciar Sistema o Cerrar Sesión)

1. **shutdown -h now**: apagar el sistema (1).
2. **init 0**: apagar el sistema (2).
3. **telinit 0**: apagar el sistema (3).
4. **halt**: apagar el sistema (4).
5. **shutdown -h hours:minutes &**: apagado planificado del sistema.
6. **shutdown -c**: cancelar un apagado planificado del sistema.
7. **shutdown -r now**: reiniciar (1).
8. **reboot**: reiniciar (2).
9. **logout**: cerrar sesión.

Archivos y Directorios

1. **cd /home**: entrar en el directorio "home".
2. **cd ..**: retroceder un nivel.
3. **cd ../..**: retroceder 2 niveles.
4. **cd:** ir al directorio raíz.
5. **cd ~user1**: ir al directorio user1.
6. **cd -**: ir (regresar) al directorio anterior.
7. **pwd**: mostrar el camino del directorio de trabajo.
8. **ls**: ver los ficheros de un directorio.
9. **ls -F**: ver los ficheros de un directorio.
10. **ls -l**: mostrar los detalles de ficheros y carpetas de un directorio.
11. **ls -a**: mostrar los ficheros ocultos.
12. **ls *[0-9]***: mostrar los ficheros y carpetas que contienen números.
13. **tree**: mostrar los ficheros y carpetas en forma de árbol comenzando por la raíz.(1)
14. **lstree**: mostrar los ficheros y carpetas en forma de árbol comenzando por la raíz.(2)
15. **mkdir dir1**: crear una carpeta o directorio con nombre 'dir1?.
16. **mkdir dir1 dir2**: crear dos carpetas o directorios simultáneamente (Crear dos directorios a la vez).
17. **mkdir -p /tmp/dir1/dir2**: crear un árbol de directorios.
18. **rm -f file1**: borrar el fichero llamado 'file1?.
19. **rmdir dir1**: borrar la carpeta llamada 'dir1?.
20. **rm -rf dir1**: eliminar una carpeta llamada 'dir1? con su contenido de forma recursiva. (Si lo borro recursivo estoy diciendo que es con su contenido).
21. **rm -rf dir1 dir2**: borrar dos carpetas (directorios) con su contenido de forma recursiva.
22. **mv dir1 new_dir**: renombrar o mover un fichero o carpeta (directorio).
23. **cp file1**: copiar un fichero.
24. **cp file1 file2**: copiar dos ficheros al unísono.
25. **cp dir /* .**: copiar todos los ficheros de un directorio dentro del directorio de trabajo actual.
26. **cp -a /tmp/dir1 .**: copiar un directorio dentro del directorio actual de trabajo.
27. **cp -a dir1**: copiar un directorio.
28. **cp -a dir1 dir2**: copiar dos directorio al unísono.
29. **ln -s file1 lnk1**: crear un enlace simbólico al fichero o directorio.
30. **ln file1 lnk1**: crear un enlace físico al fichero o directorio.
31. **touch -t 0712250000 file1**: modificar el tiempo real (tiempo de creación) de un fichero o directorio.
32. **file file1**: salida (volcado en pantalla) del tipo mime de un fichero texto.
33. **iconv -l**: listas de cifrados conocidos.
34. **iconv -f fromEncoding -t toEncoding inputFile > outputFile**: crea una nueva forma del fichero de entrada asumiendo que está codificado en fromEncoding y convirtiéndolo a ToEncoding.
35. **find . -maxdepth 1 -name *.jpg -print -exec convert "{}" -resize 80×60 "thumbs/{}" \;**: agrupar ficheros redimensionados en el directorio actual y enviarlos a directorios en vistas de miniaturas (requiere convertir desde ImagemagicK).

Encontrar archivos

► enero (6)

► 2012 (93)
► 2011 (72)
► 2010 (195)
► 2009 (163)

3nlaces:

[A]NTRAX-[L]ABS

Foro Underc0de

Kitploit - The Hacker's Tools

Sunploit

Th3 R4v3n

Daily Picture

1. **find / -name file1**: buscar fichero y directorio a partir de la raíz del sistema.
2. **find / -user user1**: buscar ficheros y directorios pertenecientes al usuario 'user1?.
3. **find /home/user1 -name *.bin**: buscar ficheros con extensión '. bin' dentro del directorio '/ home/user1?.
4. **find /usr/bin -type f -atime +100**: buscar ficheros binarios no usados en los últimos 100 días.
5. **find /usr/bin -type f -mtime -10**: buscar ficheros creados o cambiados dentro de los últimos 10 días.
6. **find / -name *.rpm -exec chmod 755 '{}' \;**: buscar ficheros con extensión '.rpm' y modificar permisos.
7. **find / -xdev -name *.rpm**: Buscar ficheros con extensión '.rpm' ignorando los dispositivos removibles como cdrom, pen-drive, etc.…
8. **locate *.ps**: encuentra ficheros con extensión '.ps' ejecutados primeramente con el command 'updatedb'.
9. **whereis halt**: mostrar la ubicación de un fichero binario, de ayuda o fuente. En este caso pregunta dónde está el comando 'halt'.
10. **which halt**: mostrar la senda completa (el camino completo) a un binario / ejecutable.

Montando un sistema de ficheros

1. **mount /dev/hda2 /mnt/hda2**: montar un disco llamado hda2. Verifique primero la existencia del directorio '/ mnt/hda2?; si no está, debe crearlo.
2. **umount /dev/hda2**: desmontar un disco llamado hda2. Salir primero desde el punto '/ mnt/hda2.
3. **fuser -km /mnt/hda2**: forzar el desmontaje cuando el dispositivo está ocupado.
4. **umount -n /mnt/hda2**: correr el desmontaje sin leer el fichero /etc/mtab. Útil cuando el fichero es de solo lectura o el disco duro está lleno.
5. **mount /dev/fd0 /mnt/floppy**: montar un disco flexible (floppy).
6. **mount /dev/cdrom /mnt/cdrom**: montar un cdrom / dvdrom.
7. **mount /dev/hdc /mnt/cdrecorder**: montar un cd regrabable o un dvdrom.
8. **mount /dev/hdb /mnt/cdrecorder**: montar un cd regrabable / dvdrom (un dvd).
9. **mount -o loop file.iso /mnt/cdrom**: montar un fichero o una imagen iso.
10. **mount -t vfat /dev/hda5 /mnt/hda5**: montar un sistema de ficheros FAT32.
11. **mount /dev/sda1 /mnt/usbdisk**: montar un usb pen-drive o una memoria (sin especificar el tipo de sistema de ficheros).

Espacio de Disco

1. **df -h**: mostrar una lista de las particiones montadas.
2. **ls -lSr |more**: mostrar el tamaño de los ficheros y directorios ordenados por tamaño.
3. **du -sh dir1**: Estimar el espacio usado por el directorio 'dir1?.
4. **du -sk * | sort -rn**: mostrar el tamaño de los ficheros y directorios ordenados por tamaño.
5. **rpm -q -a –qf '%10{SIZE}t%{NAME}n' | sort -k1,1n**: mostrar el espacio usado por los paquetes rpm instalados organizados por tamaño (Fedora, Redhat y otros).
6. **dpkg-query -W -f='${Installed-Size;10}t${Package}n' | sort -k1,1n**: mostrar el espacio usado por los paquetes instalados, organizados por tamaño (Ubuntu, Debian y otros).

Usuarios y Grupos

1. **groupadd nombre_del_grupo**: crear un nuevo grupo.
2. **groupdel nombre_del_grupo**: borrar un grupo.
3. **groupmod -n nuevo_nombre_del_grupo viejo_nombre_del_grupo**: renombrar un grupo.
4. **useradd -c "Name Surname " -g admin -d /home/user1 -s /bin/bash user1**: Crear un nuevo usuario perteneciente al grupo "admin".
5. **useradd user1**: crear un nuevo usuario.
6. **userdel -r user1**: borrar un usuario ('-r' elimina el directorio Home).
7. **usermod -c "User FTP" -g system -d /ftp/user1 -s /bin/nologin user1**: cambiar los atributos del usuario.
8. **passwd**: cambiar contraseña.
9. **passwd user1**: cambiar la contraseña de un usuario (solamente por root).
10. **chage -E 2011-12-31 user1**: colocar un plazo para la contraseña del usuario. En este caso dice que la clave expira el 31 de diciembre de 2011.
11. **pwck**: chequear la sintaxis correcta el formato de fichero de '/etc/passwd' y la existencia de usuarios.
12. **grpck**: chequear la sintaxis correcta y el formato del fichero '/etc/group' y la existencia de grupos.
13. **newgrp group_name**: registra a un nuevo grupo para cambiar el grupo predeterminado de los ficheros creados recientemente.

Permisos en Ficheros (Usa "+" para colocar permisos y "-" para eliminar)

1. **ls -lh**: Mostrar permisos.
2. **ls /tmp | pr -T5 -W$COLUMNS**: dividir la terminal en 5 columnas.
3. **chmod ugo+rwx directory1**: colocar permisos de lectura ®, escritura (w) y ejecución(x) al propietario (u), al grupo (g) y a otros (o) sobre el directorio 'directory1?.
4. **chmod go-rwx directory1**: quitar permiso de lectura ®, escritura (w) y (x) ejecución al grupo (g) y otros (o) sobre el directorio 'directory1?.
5. **chown user1 file1**: cambiar el dueño de un fichero.

6. **chown -R user1 directory1**: cambiar el propietario de un directorio y de todos los ficheros y directorios contenidos dentro.
7. **chgrp group1 file1**: cambiar grupo de ficheros.
8. **chown user1:group1 file1**: cambiar usuario y el grupo propietario de un fichero.
9. **find / -perm -u+s**: visualizar todos los ficheros del sistema con SUID configurado.
10. **chmod u+s /bin/file1**: colocar el bit SUID en un fichero binario. El usuario que corriendo ese fichero adquiere los mismos privilegios como dueño.
11. **chmod u-s /bin/file1**: deshabilitar el bit SUID en un fichero binario.
12. **chmod g+s /home/public**: colocar un bit SGID en un directorio –similar al SUID pero por directorio.
13. **chmod g-s /home/public**: desabilitar un bit SGID en un directorio.
14. **chmod o+t /home/public**: colocar un bit STIKY en un directorio. Permite el borrado de ficheros solamente a los dueños legítimos.
15. **chmod o-t /home/public**: desabilitar un bit STIKY en un directorio.

Atributos especiales en ficheros (Usa "+" para colocar permisos y "-" para eliminar)

1. **chattr +a file1**: permite escribir abriendo un fichero solamente modo append.
2. **chattr +c file1**: permite que un fichero sea comprimido / descomprimido automaticamente.
3. **chattr +d file1**: asegura que el programa ignore borrar los ficheros durante la copia de seguridad.
4. **chattr +i file1**: convierte el fichero en invariable, por lo que no puede ser eliminado, alterado, renombrado, ni enlazado.
5. **chattr +s file1**: permite que un fichero sea borrado de forma segura.
6. **chattr +S file1**: asegura que un fichero sea modificado, los cambios son escritos en modo synchronous como con sync.
7. **chattr +u file1**: te permite recuperar el contenido de un fichero aún si este está cancelado.
8. **lsattr**: mostrar atributos especiales.

Archivos y Ficheros comprimidos

1. **bunzip2 file1.bz2**: descomprime in fichero llamado 'file1.bz2?.
2. **bzip2 file1**: comprime un fichero llamado 'file1?.
3. **gunzip file1.gz**: descomprime un fichero llamado 'file1.gz'.
4. **gzip file1**: comprime un fichero llamado 'file1?.
5. **gzip -9 file1**: comprime con compresión máxima.
6. **rar a file1.rar test_file**: crear un fichero rar llamado 'file1.rar'.
7. **rar a file1.rar file1 file2 dir1**: comprimir 'file1?, 'file2? y 'dir1? simultáneamente.
8. **rar x file1.rar**: descomprimir archivo rar.
9. **unrar x file1.rar**: descomprimir archivo rar.
10. **tar -cvf archive.tar file1**: crear un tarball descomprimido.
11. **tar -cvf archive.tar file1 file2 dir1**: crear un archivo conteniendo 'file1?, 'file2? y'dir1?.
12. **tar -tf archive.tar**: mostrar los contenidos de un archivo.
13. **tar -xvf archive.tar**: extraer un tarball.
14. **tar -xvf archive.tar -C /tmp**: extraer un tarball en / tmp.
15. **tar -cvfj archive.tar.bz2 dir1**: crear un tarball comprimido dentro de bzip2.
16. **tar -xvfj archive.tar.bz2**: descomprimir un archivo tar comprimido en bzip2
17. **tar -cvfz archive.tar.gz dir1**: crear un tarball comprimido en gzip.
18. **tar -xvfz archive.tar.gz**: descomprimir un archive tar comprimido en gzip.
19. **zip file1.zip file1**: crear un archivo comprimido en zip.
20. **zip -r file1.zip file1 file2 dir1**: comprimir, en zip, varios archivos y directorios de forma simultánea.
21. **unzip file1.zip**: descomprimir un archivo zip.

Paquetes RPM (Red Hat, Fedora y similares)

1. **rpm -ivh package.rpm**: instalar un paquete rpm.
2. **rpm -ivh –nodeeps package.rpm**: instalar un paquete rpm ignorando las peticiones de dependencias.
3. **rpm -U package.rpm**: actualizar un paquete rpm sin cambiar la configuración de los ficheros.
4. **rpm -F package.rpm**: actualizar un paquete rpm solamente si este está instalado.
5. **rpm -e package_name.rpm**: eliminar un paquete rpm.
6. **rpm -qa**: mostrar todos los paquetes rpm instalados en el sistema.
7. **rpm -qa | grep httpd**: mostrar todos los paquetes rpm con el nombre "httpd".
8. **rpm -qi package_name**: obtener información en un paquete específico instalado.
9. **rpm -qg "System Environment/Daemons"**: mostar los paquetes rpm de un grupo software.
10. **rpm -ql package_name**: mostrar lista de ficheros dados por un paquete rpm instalado.
11. **rpm -qc package_name**: mostrar lista de configuración de ficheros dados por un paquete rpm instalado.
12. **rpm -q package_name –whatrequires**: mostrar lista de dependencias solicitada para un paquete rpm.
13. **rpm -q package_name –whatprovides**: mostar la capacidad dada por un paquete rpm.
14. **rpm -q package_name –scripts**: mostrar los scripts comenzados durante la instalación /eliminación.
15. **rpm -q package_name –changelog**: mostar el historial de revisions de un paquete rpm.

16. **rpm -qf /etc/httpd/conf/httpd.conf**: verificar cuál paquete rpm pertenece a un fichero dado.
17. **rpm -qp package.rpm -l**: mostrar lista de ficheros dados por un paquete rpm que aún no ha sido instalado.
18. **rpm –import /media/cdrom/RPM-GPG-KEY**: importar la firma digital de la llave pública.
19. **rpm –checksig package.rpm**: verificar la integridad de un paquete rpm.
20. **rpm -qa gpg-pubkey**: verificar la integridad de todos los paquetes rpm instalados.
21. **rpm -V package_name**: chequear el tamaño del fichero, licencias, tipos, dueño, grupo, chequeo de resumen de MD5 y última modificación.
22. **rpm -Va**: chequear todos los paquetes rpm instalados en el sistema. Usar con cuidado.
23. **rpm -Vp package.rpm**: verificar un paquete rpm no instalado todavía.
24. **rpm2cpio package.rpm | cpio –extract –make-directories *bin***: extraer fichero ejecutable desde un paquete rpm.
25. **rpm -ivh /usr/src/redhat/RPMS/`arch`/package.rpm**: instalar un paquete construido desde una fuente rpm.
26. **rpmbuild –rebuild package_name.src.rpm**: construir un paquete rpm desde una fuente rpm.

Actualizador de paquetes YUM (Red Hat, Fedora y similares)

1. **yum install package_name**: descargar e instalar un paquete rpm.
2. **yum localinstall package_name.rpm**: este instalará un RPM y tratará de resolver todas las dependencies para ti, usando tus repositorios.
3. **yum update package_name.rpm**: actualizar todos los paquetes rpm instalados en el sistema.
4. **yum update package_name**: modernizar / actualizar un paquete rpm.
5. **yum remove package_name**: eliminar un paquete rpm.
6. **yum list**: listar todos los paquetes instalados en el sistema.
7. **yum search package_name**: Encontrar un paquete en repositorio rpm.
8. **yum clean packages**: limpiar un caché rpm borrando los paquetes descargados.
9. **yum clean headers**: eliminar todos los ficheros de encabezamiento que el sistema usa para resolver la dependencia.
10. **yum clean all**: eliminar desde los paquetes caché y ficheros de encabezado.

Paquetes Deb (Debian, Ubuntu y derivados)

1. **dpkg -i package.deb**: instalar / actualizar un paquete deb.
2. **dpkg -r package_name**: eliminar un paquete deb del sistema.
3. **dpkg -l**: mostrar todos los paquetes deb instalados en el sistema.
4. **dpkg -l | grep httpd**: mostrar todos los paquetes deb con el nombre “httpd”
5. **dpkg -s package_name**: obtener información en un paquete específico instalado en el sistema.
6. **dpkg -L package_name**: mostar lista de ficheros dados por un paquete instalado en el sistema.
7. **dpkg –contents package.deb**: mostrar lista de ficheros dados por un paquete no instalado todavía.
8. **dpkg -S /bin/ping**: verificar cuál paquete pertenece a un fichero dado.

Actualizador de paquetes APT (Debian, Ubuntu y derivados)

1. **apt-get install package_name**: instalar / actualizar un paquete deb.
2. **apt-cdrom install package_name**: instalar / actualizar un paquete deb desde un cdrom.
3. **apt-get update**: actualizar la lista de paquetes.
4. **apt-get upgrade**: actualizar todos los paquetes instalados.
5. **apt-get remove package_name**: eliminar un paquete deb del sistema.
6. **apt-get check**: verificar la correcta resolución de las dependencias.
7. **apt-get clean**: limpiar cache desde los paquetes descargados.
8. **apt-cache search searched-package**: retorna lista de paquetes que corresponde a la serie «paquetes buscados».

Ver el contenido de un fichero

1. **cat file1**: ver los contenidos de un fichero comenzando desde la primera hilera.
2. **tac file1**: ver los contenidos de un fichero comenzando desde la última línea.
3. **more file1**: ver el contenido a lo largo de un fichero.
4. **less file1**: parecido al commando ‘more’ pero permite salvar el movimiento en el fichero así como el movimiento hacia atrás.
5. **head -2 file1**: ver las dos primeras líneas de un fichero.
6. **tail -2 file1**: ver las dos últimas líneas de un fichero.
7. **tail -f /var/log/messages**: ver en tiempo real qué ha sido añadido al fichero.

Manipulación de texto

1. **cat file1 file2 .. | command <> file1_in.txt_or_file1_out.txt**: sintaxis general para la manipulación de texto utilizando PIPE, STDIN y STDOUT.
2. **cat file1 | command(sed, grep, awk, grep, etc…) > result.txt**: sintaxis general para manipular un texto de un fichero y escribir el resultado en un fichero nuevo.

3. **cat file1 | command(sed, grep, awk, grep, etc…) » result.txt**: sintaxis general para manipular un texto de un fichero y añadir resultado en un fichero existente.
4. **grep Aug /var/log/messages**: buscar palabras “Aug” en el fichero ‘/var/log/messages’.
5. **grep ^Aug /var/log/messages**: buscar palabras que comienzan con “Aug” en fichero ‘/var/log/messages’
6. **grep [0-9] /var/log/messages**: seleccionar todas las líneas del fichero ‘/var/log/messages’ que contienen números.
7. **grep Aug -R /var/log/***: buscar la cadena “Aug” en el directorio ‘/var/log’ y debajo.
8. **sed ‘s/stringa1/stringa2/g’ example.txt**: reubicar “string1” con “string2” en ejemplo.txt
9. **sed ‘/^$/d’ example.txt**: eliminar todas las líneas en blanco desde el ejemplo.txt
10. **sed ‘/ *#/d; /^$/d’ example.txt**: eliminar comentarios y líneas en blanco de ejemplo.txt
11. **echo ‘esempio’ | tr ‘[:lower:]‘ ‘[:upper:]‘**: convertir minúsculas en mayúsculas.
12. **sed -e ’1d’ result.txt**: elimina la primera línea del fichero ejemplo.txt
13. **sed -n ‘/stringa1/p’**: visualizar solamente las líneas que contienen la palabra “string1”.

Establecer caracter y conversión de ficheros

1. **dos2unix filedos.txt fileunix.txt**: convertir un formato de fichero texto desde MSDOS a UNIX.
2. **unix2dos fileunix.txt filedos.txt**: convertir un formato de fichero de texto desde UNIX a MSDOS.
3. **recode ..HTML < page.txt > page.html**: convertir un fichero de texto en html.
4. **recode -l | more**: mostrar todas las conversiones de formato disponibles.

Análisis del sistema de ficheros

1. **badblocks -v /dev/hda1**: Chequear los bloques defectuosos en el disco hda1.
2. **fsck /dev/hda1**: reparar / chequear la integridad del fichero del sistema Linux en el disco hda1.
3. **fsck.ext2 /dev/hda1**: reparar / chequear la integridad del fichero del sistema ext 2 en el disco hda1.
4. **e2fsck /dev/hda1**: reparar / chequear la integridad del fichero del sistema ext 2 en el disco hda1.
5. **e2fsck -j /dev/hda1**: reparar / chequear la integridad del fichero del sistema ext 3 en el disco hda1.
6. **fsck.ext3 /dev/hda1**: reparar / chequear la integridad del fichero del sistema ext 3 en el disco hda1.
7. **fsck.vfat /dev/hda1**: reparar / chequear la integridad del fichero sistema fat en el disco hda1.
8. **fsck.msdos /dev/hda1**: reparar / chequear la integridad de un fichero del sistema dos en el disco hda1.
9. **dosfsck /dev/hda1**: reparar / chequear la integridad de un fichero del sistema dos en el disco hda1.

Formatear un sistema de ficheros

1. **mkfs /dev/hda1**: crear un fichero de sistema tipo Linux en la partición hda1.
2. **mke2fs /dev/hda1**: crear un fichero de sistema tipo Linux ext 2 en hda1.
3. **mke2fs -j /dev/hda1**: crear un fichero de sistema tipo Linux ext3 (periódico) en la partición hda1.
4. **mkfs -t vfat 32 -F /dev/hda1**: crear un fichero de sistema FAT32 en hda1.
5. **fdformat -n /dev/fd0**: formatear un disco flooply.
6. **mkswap /dev/hda3**: crear un fichero de sistema swap.

Trabajo con la SWAP

1. **mkswap /dev/hda3**: crear fichero de sistema swap.
2. **swapon /dev/hda3**: activando una nueva partición swap.
3. **swapon /dev/hda2 /dev/hdb3**: activar dos particiones swap.

Salvas (Backup)

1. **dump -0aj -f /tmp/home0.bak /home**: hacer una salva completa del directorio ‘/home’.
2. **dump -1aj -f /tmp/home0.bak /home**: hacer una salva incremental del directorio ‘/home’.
3. **restore -if /tmp/home0.bak**: restaurando una salva interactivamente.
4. **rsync -rogpav –delete /home /tmp**: sincronización entre directorios.
5. **rsync -rogpav -e ssh –delete /home ip_address:/tmp**: rsync a través del túnel SSH.
6. **rsync -az -e ssh –delete ip_addr:/home/public /home/local**: sincronizar un directorio local con un directorio remoto a través de ssh y de compresión.
7. **rsync -az -e ssh –delete /home/local ip_addr:/home/public**: sincronizar un directorio remoto con un directorio local a través de ssh y de compresión.
8. **dd bs=1M if=/dev/hda | gzip | ssh user@ip_addr ‘dd of=hda.gz’**: hacer una salva de un disco duro en un host remoto a través de ssh.
9. **dd if=/dev/sda of=/tmp/file1**: salvar el contenido de un disco duro a un fichero. (En este caso el disco duro es “sda” y el fichero “file1”).
10. **tar -Puf backup.tar /home/user**: hacer una salva incremental del directorio ‘/home/user’.
11. **(cd /tmp/local/ && tar c .) | ssh -C user@ip_addr ‘cd /home/share/ && tar x -p’**: copiar el contenido de un directorio en un directorio remoto a través de ssh.
12. **(tar c /home) | ssh -C user@ip_addr ‘cd /home/backup-home && tar x -p’**: copiar un directorio local en un directorio remoto a través de ssh.
13. **tar cf – . | (cd /tmp/backup ; tar xf –)**: copia local conservando las licencias y enlaces desde un directorio a otro.

14. **find /home/user1 -name '*.txt' | xargs cp -av –target-directory=/home/backup/ –parents**: encontrar y copiar todos los ficheros con extensión '.txt' de un directorio a otro.
15. **find /var/log -name '*.log' | tar cv –files-from=- | bzip2 > log.tar.bz2**: encontrar todos los ficheros con extensión '.log' y hacer un archivo bzip.
16. **dd if=/dev/hda of=/dev/fd0 bs=512 count=1**: hacer una copia del MRB (Master Boot Record) a un disco floppy.
17. **dd if=/dev/fd0 of=/dev/hda bs=512 count=1**: restaurar la copia del MBR (Master Boot Record) salvada en un floppy.

CD-ROM

1. **cdrecord -v gracetime=2 dev=/dev/cdrom -eject blank=fast -force**: limpiar o borrar un cd regrabable.
2. **mkisofs /dev/cdrom > cd.iso**: crear una imagen iso de cdrom en disco.
3. **mkisofs /dev/cdrom | gzip > cd_iso.gz**: crear una imagen comprimida iso de cdrom en disco.
4. **mkisofs -J -allow-leading-dots -R -V "Label CD" -iso-level 4 -o ./cd.iso data_cd**: crear una imagen iso de un directorio.
5. **cdrecord -v dev=/dev/cdrom cd.iso**: quemar una imagen iso.
6. **gzip -dc cd_iso.gz | cdrecord dev=/dev/cdrom -**: quemar una imagen iso comprimida.
7. **mount -o loop cd.iso /mnt/iso**: montar una imagen iso.
8. **cd-paranoia -B**: llevar canciones de un cd a ficheros wav.
9. **cd-paranoia – "-3"**: llevar las 3 primeras canciones de un cd a ficheros wav.
10. **cdrecord –scanbus**: escanear bus para identificar el canal scsi.
11. **dd if=/dev/hdc | md5sum**: hacer funcionar un md5sum en un dispositivo, como un CD.

Trabajo con la RED (LAN y Wi-Fi)

1. **ifconfig eth0**: mostrar la configuración de una tarjeta de red Ethernet.
2. **ifup eth0**: activar una interface 'eth0?.
3. **ifdown eth0**: deshabilitar una interface 'eth0?.
4. **ifconfig eth0 192.168.1.1 netmask 255.255.255.0**: configurar una dirección IP.
5. **ifconfig eth0 promisc**: configurar 'eth0?en modo común para obtener los paquetes (sniffing).
6. **dhclient eth0**: activar la interface 'eth0? en modo dhcp.
7. **route -n**: mostrar mesa de recorrido.
8. **route add -net 0/0 gw IP_Gateway**: configurar entrada predeterminada.
9. **route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1**: configurar ruta estática para buscar la red '192.168.0.0/16?.
10. **route del 0/0 gw IP_gateway**: eliminar la ruta estática.
11. **echo "1" > /proc/sys/net/ipv4/ip_forward**: activar el recorrido ip.
12. **hostname**: mostrar el nombre del host del sistema.
13. **host www.example.com**: buscar el nombre del host para resolver el nombre a una dirección ip(1).
14. **nslookup www.example.com**: buscar el nombre del host para resolver el nombre a una direccióm ip y viceversa(2).
15. **ip link show**: mostar el estado de enlace de todas las interfaces.
16. **mii-tool eth0**: mostar el estado de enlace de 'eth0?.
17. **ethtool eth0**: mostrar las estadísticas de tarjeta de red 'eth0?.
18. **netstat -tup**: mostrar todas las conexiones de red activas y sus PID.
19. **netstat -tupl**: mostrar todos los servicios de escucha de red en el sistema y sus PID.
20. **tcpdump tcp port 80**: mostrar todo el tráfico HTTP.
21. **iwlist scan**: mostrar las redes inalámbricas.
22. **iwconfig eth1**: mostrar la configuración de una tarjeta de red inalámbrica.
23. **whois www.example.com**: buscar en base de datos Whois.

Redes de Microsoft Windows (SAMBA)

1. **nbtscan ip_addr**: resolución de nombre de red bios.
2. **nmblookup -A ip_addr**: resolución de nombre de red bios.
3. **smbclient -L ip_addr/hostname**: mostrar acciones remotas de un host en windows.

Tablas IP (CORTAFUEGOS)

1. **iptables -t filter -L**: mostrar todas las cadenas de la tabla de filtro.
2. **iptables -t nat -L**: mostrar todas las cadenas de la tabla nat.
3. **iptables -t filter -F**: limpiar todas las reglas de la tabla de filtro.
4. **iptables -t nat -F**: limpiar todas las reglas de la tabla nat.
5. **iptables -t filter -X**: borrar cualquier cadena creada por el usuario.
6. **iptables -t filter -A INPUT -p tcp –dport telnet -j ACCEPT**: permitir las conexiones telnet para entar.
7. **iptables -t filter -A OUTPUT -p tcp –dport http -j DROP**: bloquear las conexiones HTTP para salir.
8. **iptables -t filter -A FORWARD -p tcp –dport pop3 -j ACCEPT**: permitir las conexiones POP a una cadena delantera.
9. **iptables -t filter -A INPUT -j LOG –log-prefix "DROP INPUT"**: registrando una cadena de entrada.



10. **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**: configurar un PAT (Puerto de traducción de dirección) en eth0, ocultando los paquetes de salida forzada.
11. **iptables -t nat -A PREROUTING -d 192.168.0.1 -p tcp -m tcp –dport 22 -j DNAT –to-destination 10.0.0.2:22**: redireccionar los paquetes diriguidos de un host a otro.

Monitoreando y depurando

1. **top**: mostrar las tareas de linux usando la mayoría cpu.
2. **ps -eafw**: muestra las tareas Linux.
3. **ps -e -o pid,args –forest**: muestra las tareas Linux en un modo jerárquico.
4. **pstree**: mostrar un árbol sistema de procesos.
5. **kill -9 ID_Processo**: forzar el cierre de un proceso y terminarlo.
6. **kill -1 ID_Processo**: forzar un proceso para recargar la configuración.
7. **lsof -p $$**: mostrar una lista de ficheros abiertos por procesos.
8. **lsof /home/user1**: muestra una lista de ficheros abiertos en un camino dado del sistema.
9. **strace -c ls >/dev/null**: mostrar las llamadas del sistema hechas y recibidas por un proceso.
10. **strace -f -e open ls >/dev/null**: mostrar las llamadas a la biblioteca.
11. **watch -n1 'cat /proc/interrupts'**: mostrar interrupciones en tiempo real.
12. **last reboot**: mostrar historial de reinicio.
13. **lsmod**: mostrar el kernel cargado.
14. **free -m**: muestra el estado de la RAM en megabytes.
15. **smartctl -A /dev/hda**: monitorear la fiabilidad de un disco duro a través de SMART.
16. **smartctl -i /dev/hda**: chequear si SMART está activado en un disco duro.
17. **tail /var/log/dmesg**: mostrar eventos inherentes al proceso de carga del kernel.
18. **tail /var/log/messages**: mostrar los eventos del sistema.

Otros comandos útiles

1. **apropos …keyword**: mostrar una lista de comandos que pertenecen a las palabras claves de un programa; son útiles cuando tú sabes qué hace tu programa, pero de sconoces el nombre del comando.
2. **man ping**: mostrar las páginas del manual on-line; por ejemplo, en un comando ping, usar la opción '-k' para encontrar cualquier comando relacionado.
3. **whatis …keyword**: muestra la descripción de lo que hace el programa.
4. **mkbootdisk –device /dev/fd0 `uname -r`**: crear un floppy boteable.
5. **gpg -c file1**: codificar un fichero con guardia de seguridad GNU.
6. **gpg file1.gpg**: decodificar un fichero con Guardia de seguridad GNU.
7. **wget -r www.example.com**: descargar un sitio web completo.
8. **wget -c www.example.com/file.iso**: descargar un fichero con la posibilidad de parar la descargar y reanudar más tarde.
9. **echo 'wget -c www.example.com/files.iso' | at 09:00**: Comenzar una descarga a cualquier hora. En este caso empezaría a las 9 horas.
10. **ldd /usr/bin/ssh**: mostrar las bibliotecas compartidas requeridas por el programa ssh.
11. **alias hh='history'**: colocar un alias para un commando –hh= Historial.
12. **chsh**: cambiar el comando Shell.
13. **chsh –list-shells**: es un comando adecuado para saber si tienes que hacer remoto en otra terminal.
14. **who -a**: mostrar quien está registrado, e imprimir hora del último sistema de importación, procesos muertos, procesos de registro de sistema, procesos activos producidos por init, funcionamiento actual y últimos cambios del reloj del sistema.

Fuente: http://gutl.jovenclub.cu/

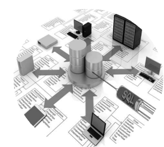
What's Related?



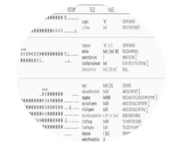
Obtener Contraseñas de Hotmail, Yah...



Hackers&Developers Revista de Softw...



SQL Injection Cheat Sheet



Estructura Interna de los Ficheros ...



Recopilación de PDFs sobre Segurida...

Author & Editor